Свойства символа Лежандра

Свойство 1: $(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \pmod{p}, p \neq 2$

Свойства символа Лежандра

Свойство 1: $(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \pmod p, p \neq 2$

Отметим, что $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p \Leftrightarrow a^{p-1} - 1 \equiv 0.$

Свойства символа Лежандра

Свойство 1: $(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \pmod p, p \neq 2$

Отметим, что $(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \pmod p \Leftrightarrow a^{p-1}-1 \equiv 0.$

Следовательно: $(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0(1).$

Если a – кв. вычет, то $\exists x : a = x^2 \Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1$

Свойства символа Лежандра

Свойство 1: $(\frac{a}{b}) \equiv a^{\frac{p-1}{2}} \pmod p, p \neq 2$

Отметим, что $(a,p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p \Leftrightarrow a^{p-1} - 1 \equiv 0$.

Следовательно: $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0(1)$.

Если a – кв. вычет, то $\exists x : a = x^2 \Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1$

Если a – вычет, то (1) обращаеця в 0, но вычетов у нас $\frac{p-1}{2}$ (корни сравнения), значит корни второй скобки из (1) будут невычетами.

Лемма 6

$(p, a) = 1, p_1 = \frac{p-1}{2}$ и $r_i \in [-p_1, p_1] \setminus \{0\}$.

$1 \cdot a \equiv \epsilon_1 \cdot r_1$

$2 \cdot a \equiv \epsilon_2 \cdot r_2$

$\ldots$

$p_1 \cdot a \equiv \epsilon_{p_1} \cdot r_{p_1}$

Лемма 6

$(p, a) = 1, p_1 = \frac{p-1}{2}$ и $r_i \in [-p_1, p_1] \setminus \{0\}$.

$1 \cdot a \equiv \epsilon_1 \cdot r_1$

$2 \cdot a \equiv \epsilon_2 \cdot r_2$

$\dots$

$p_1 \cdot a \equiv \epsilon_{p_1} \cdot r_{p_1}$

Перемножим сравнения: $p_1! a^{p_1} \equiv \epsilon_1 \dots \epsilon_{p_1} \cdot p_1!$.

Т.к. остатки это в точности те же самые числа, что и коэффициенты перед a.

Лемма 6

$(p, a) = 1, p_1 = \frac{p-1}{2}$ и $r_i \in [-p_1, p_1] \setminus \{0\}$.

$1 \cdot a \equiv \epsilon_1 \cdot r_1$

$2 \cdot a \equiv \epsilon_2 \cdot r_2$
$\dots$
$p_1 \cdot a \equiv \epsilon_{p_1} \cdot r_{p_1}$

Перемножим сравнения: $p_1! a^{p_1} \equiv \epsilon_1 \dots \epsilon_{p_1} \cdot p_1!$.

Т.к. остатки это в точности те же самые числа, что и коэффициенты перед a.

Тогда можно сократить на $p_1!$ и получить $a^{p_1} \equiv \epsilon_1 \dots \epsilon_{p_1}$.

Лемма 6

$(p, a) = 1, p_1 = \frac{p-1}{2}$ и $r_i \in [-p_1, p_1] \setminus \{0\}$.

$1 \cdot a \equiv \epsilon_1 \cdot r_1$

$2 \cdot a \equiv \epsilon_2 \cdot r_2$

$\ldots$

$p_1 \cdot a \equiv \epsilon_{p_1} \cdot r_{p_1}$

Перемножим сравнения: $p_1! a^{p_1} \equiv \epsilon_1 \ldots \epsilon_{p_1} \cdot p_1!$.

Т.к. остатки это в точности те же самые числа, что и коэффициенты перед a.

Тогда можно сократить на $p_1!$ и получить $a^{p_1} \equiv \epsilon_1 \ldots \epsilon_{p_1}$.

Докажем этот факт. Пусть есть одинаковые остатки, тогда $ia \equiv ja$.

$a(i - j) \equiv 0 \Rightarrow i - j \vdots p$, что не так, так как $i < j \leq p_1$.

Аналогично с $ia \equiv -ja$.

Лемма 6

$$(-1)^{[\frac{2ax}{p}]} = (-1)^{[[\frac{2ax}{p}]+\{\frac{2ax}{p}\}]} = (-1)^{2[\frac{ax}{p}]+[2\{\frac{ax}{p}\}]}.$$

Так как $2[\frac{ax}{p}] \vdots 2$: $(-1)^{[2\{\frac{ax}{p}\}]} = \epsilon_x$

Лемма 6

$(-1)^{[\frac{2ax}{p}]} = (-1)^{[[\frac{2ax}{p}]+\{\frac{2ax}{p}\}]} = (-1)^{2[\frac{ax}{p}]+[2\{\frac{ax}{p}\}]}.$

Так как $2[\frac{ax}{p}] \vdots 2$: $(-1)^{[2\{\frac{ax}{p}\}]} = \epsilon_x$

$ax \equiv \epsilon_x \cdot r_x.$

$\epsilon_x = 1$, если $\frac{ax}{p} < \frac{1}{2}$.

Лемма 6

$(-1)^{[\frac{2ax}{p}]} = (-1)^{[[\frac{2ax}{p}]+\{\frac{2ax}{p}\}]} = (-1)^{2[\frac{ax}{p}]+[2\{\frac{ax}{p}\}]}.$

Так как $2[\frac{ax}{p}] \vdots 2$: $(-1)^{[2\{\frac{ax}{p}\}]} = \epsilon_x$

$ax \equiv \epsilon_x \cdot r_x.$

$\epsilon_x = 1$, если $\frac{ax}{p} < \frac{1}{2}$.

$$(\frac{a}{p}) \equiv a^{p_1} \equiv \epsilon_1 \dots \epsilon_{p_1} = (-1)^{\sum\limits_{x=1}^{p_1}[\frac{2ax}{p}]}.$$

ЧТД

Лемма 7

Пусть $p \in \mathbb{P}, p_1 = \frac{p-1}{2}$.

Доказем:

1) $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

2) При нечетном a получим $(\frac{a}{p}) = (-1)^{\sum\limits_{x=1}^{p_1}[\frac{ax}{p}]}$

Лемма 7

Пусть $p \in \mathbb{P}, p_1 = \frac{p-1}{2}$.

Докажем:

1) $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

2) При нечетном a получим $(\frac{a}{p}) = (-1)^{\sum\limits_{x=1}^{p_1}[\frac{ax}{p}]}$

$$(\frac{a}{p}) = (\frac{p+a}{p}) = (\frac{2\frac{p+a}{2}}{p}) = (\frac{2}{p})(\frac{\frac{p+a}{2}}{p}) = (\frac{2}{p}) \cdot (-1)^{\sum\limits_{x=1}^{p_1}[\frac{2x\frac{p+a}{2}}{p}]} =$$

$$(\frac{2}{p}) \cdot (-1)^{\sum\limits_{x=1}^{p_1}(x+[\frac{ax}{p}])} = (\frac{2}{p}) \cdot (-1)^{\sum\limits_{x=1}^{p_1}x} \cdot (-1)^{\sum\limits_{x=1}^{p_1}[\frac{ax}{p}]} =$$

$$(\frac{2}{p}) \cdot \frac{p_1(p_1+1)}{2} \cdot (-1)^{\sum\limits_{x=1}^{p_1}[\frac{ax}{p}]} = (\frac{2}{p}) \cdot \frac{p^2-1}{8} \cdot (-1)^{\sum\limits_{x=1}^{p_1}[\frac{ax}{p}]}$$

Лемма 7

Пусть $p \in \mathbb{P}, p_1 = \frac{p-1}{2}$.

Доказем:

1) $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

2) При нечетном a получим $(\frac{a}{p}) = (-1)^{\sum\limits_{x=1}^{p_1} [\frac{ax}{p}]}$

$$(\frac{a}{p}) = (\frac{p+a}{p}) = (\frac{2\frac{p+a}{2}}{p}) = (\frac{2}{p})(\frac{\frac{p+a}{2}}{p}) = (\frac{2}{p}) \cdot (-1)^{\sum\limits_{x=1}^{p_1} [\frac{2x\frac{p+a}{2}}{p}]} =$$

$$(\frac{2}{p}) \cdot (-1)^{\sum\limits_{x=1}^{p_1} (x+[\frac{ax}{p}])} = (\frac{2}{p}) \cdot (-1)^{\sum\limits_{x=1}^{p_1} x} \cdot (-1)^{\sum\limits_{x=1}^{p_1} [\frac{ax}{p}]} =$$

$$(\frac{2}{p}) \cdot \frac{p_1(p_1+1)}{2} \cdot (-1)^{\sum\limits_{x=1}^{p_1} [\frac{ax}{p}]} = (\frac{2}{p}) \cdot \frac{p^2-1}{8} \cdot (-1)^{\sum\limits_{x=1}^{p_1} [\frac{ax}{p}]}$$

Подставим $a = 1$, и тем самым докажем $(\frac{2}{p}) = \frac{p^2-1}{8}$